CHESHAM TOWN COUNCIL

INFORMATION TECHNOLOGY POLICY

STATEMENT OF PURPOSE

The purpose of this policy is to ensure that all employees and any volunteers or Members using Chesham Town Council IT have a clear understanding of what is and is not permitted. This will ensure the appropriate use of the council's equipment, safeguard the security of its IT systems and data and assist compliance with Data Protection law.

The policy should be read in conjunction with our Social Media Policy and Data Protection Policy.

POLICY COVERAGE

This policy covers the security and use of all Chesham Town Council's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Chesham Town Council's employees, Members, contractors, volunteers and other members of the public when using Chesham Town Council equipment and software.

The policy applies to all information, in whatever form, relating to Chesham Town Council's activities, and to all information handled by the council relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Chesham Town Council or on its behalf.

ACCEPTABLE USAGE

Computer Access Control

Access to the council's IT systems is controlled by the use of user IDs and passwords. All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the IT systems.

Individuals must not:

- Leave their user accounts logged in at an unattended and unlocked computer
- Leave their password unprotected
- Perform any unauthorised changes to the IT systems or information
- Attempt to access data that they are not authorised to use or access

- Exceed the limits of their authorisation or specific business needs to interrogate the system or data
- Connect any unauthorised device to the council's network or IT systems
- Store council data on any unauthorised equipment
- Give or transfer council data or software to any person or organisation outside the council without the appropriate authority to do so

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Individuals must not store personal files, such as music, video, photographs or games on council IT equipment.

Internet and Email Conditions of Use

The council's internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the council in any way, not in breach of any terms and conditions of employment and does not place the individual or the council in breach of statutory or other legal obligations. The council accepts that use of email and the internet is a valuable business tool, but that misuse of this facility can have a negative impact upon productivity and the council's reputation.

All individuals are accountable for their actions on the internet and email systems.

Internet Access Unacceptable Behaviour

In particular, the following is deemed unacceptable use or behaviour:

- Visiting sites that contain obscene, hateful, pornographic or illegal material
- Perpetrating any form of fraud, or software, film or music piracy
- Using the internet to send offensive or harassing material to other users
- Downloading commercial software or any copyrighted materials belonging to third parties, unless the download is covered or permitted under a commercial agreement or other such licence
- Hacking into unauthorised system, sites or files
- Publishing defamatory and/or knowingly false information about the council, colleagues, Members and/or customers on social networking sites, blogs, wikis, or any online publishing format
- Revealing confidential information about the council in a personal online posting, upload or transmission; including financial information and information relating to customers, business plans, policies, employees, Members and/or internal discussions
- Undertaking deliberate activities that waste council effort or networked resources
- Introducing any form of malicious software into the council network

Email Usage Unacceptable Behaviour

In particular, the following is deemed unacceptable use or behaviour:

- Distributing, disseminating or storing images, text or materials that are illegal, or might be considered indecent, pornographic or obscene
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered harassment
- Use of council communications systems to set up personal businesses or send chain letters
- Forwarding council confidential messages to external locations
- Accessing copyright information in a way that violates the copyright
- Breaking into the council's or another organisation's system or unauthorised use of a password or mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-council related matters
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste council effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

Council officers should regularly delete or archive emails when they are no longer current or required in order to restrict the size of their mailboxes and reduce the risk of incoming emails being rejected. Emails should not be kept longer than they are required in line with our Data Protection Policy.

Officers should be aware of the characteristics of spam and phishing emails and should not reply to these emails, but add the sender to their email system's Blocked Senders List.

Emails sent by employees must have an appropriate disclaimer relating to the use of the information contained within the email and will provide a link to the Council's Privacy Policy.

Council-Owned Information Held on Third-Party Web Sites

If you produce, collect and/or process council-related information in the course of your work, the information remains the property of Chesham Town Council. This includes such information stored on third party web sites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access, loss of information and data breaches, the council has the following clear desk and screen policy:

- Personal or confidential data must be protected using security features provided

- Computers must be logged off, locked or protected with a screen locking mechanism controlled by a password when unattended
- Care must be taken to ensure that confidential material and personal data is not left on printers or photocopiers
- Any printed matter containing personal or confidential data must be disposed of using cross cut shredders (please see the Records Destruction Procedure in the Records Retention Schedule for guidance on disposal of records).
- Printed material containing personal or confidential data should not be left unattended on desks.

Software
You must only use software that is authorised by the council on its computers. Authorised software must be used in accordance with the software supplier's licensing agreements.

Viruses
Centralised, automated virus detection and virus software updates have been implemented within the council. All PCs have antivirus software installed to automatically detect and remove viruses.

Individuals must not remove or disable antivirus software, or attempt to remove virus-infected files or clean up an infection other than by the use of approved council antivirus software and procedures.

Telephony (Voice) Equipment Acceptable Use
Use of council voice equipment is intended for business use. Individuals must not use the council's voice facilities for sending private communications on personal matters, except in exceptional circumstances. Individuals may receive limited private communications where such use does not affect the individual's business performance, is not detrimental to the council in any way, not in breach of any terms and conditions of employment and does not place the individual or the council in breach of statutory or other legal obligations.

Individuals must not:
- Use the council's voice equipment for conducting private business
- Make hoax or threatening calls to internal or external destinations
- Accept reverse charge calls from domestic or international operators, unless it is for business use

Actions Upon Termination of Contract
All council equipment and data, for example laptops and mobile devices, must be returned to the council at termination of contract.

All council data or intellectual property developed or gained during the period of employment remains the property of the council and must not be retained beyond

termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on council computers is the property of the council and there is no official provision for individual data privacy. However, wherever possible the council will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. The council have the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure system security and effective operation, and to protect against misuse.

The council maintains the right to examine any systems and inspect any data recorded in those systems, which includes but is not limited to internet access and email or messaging content. As a matter of compliance with this policy and meeting the regulatory requirements asked of the council, the council reserves the right to use monitoring software in order to check upon the use and content of emails. The council maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Any monitoring will be carried out in accordance with audited, controlled internal processes, current UK Data Protection law, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

Any individuals who suspect a breach of security policy must report it without delay to their line manager, or to the Town Clerk. All breaches of information security policy will be investigated and where investigations reveal misconduct, disciplinary action may follow in line with the council's Disciplinary Policy and Procedures. Breaches of the IT Policy by Members could contravene the Code of Conduct and action may result from this contravention.

MOBILE DEVICES AND BRING YOUR OWN DEVICE POLICY

Mobile devices include, but are not limited to:

- Laptop computers and netbooks
- Tablet devices
- Smartphones, etc.
- Portable storage, e.g. removable hard drives, USB memory sticks and data cards
- Portable audio visual equipment including data projectors, cameras, etc.

Use of personally-owned mobile devices to access and store council information, as well as an individual's own personal content, is commonly known as Bring Your Own

Device (BYOD).

This mobile policy applies to all council issued mobile devices and personally-owned mobile devices that are used to access council information, network of ICT facilities, including but not limited to, council information systems, email and council managed storage.

The policy applies to all officers and third parties (including but not limited to Members, contractors and volunteers) operating on behalf of the council or undertaking Chesham Town Council functions and thereby accessing the above systems, or who are provided with a council issued mobile device. These will hereafter be referred to as 'Users'.

The policy applies to use of mobile devices for business purposes at all times, both during and outside office hours and whether or not users are at their normal place of work.

This policy recognises that personally-owned mobile devices are and will be used to access council information, but makes no comment on the requirement or recommendation to do so, nor does it mandate or recommend the use of personally-owned mobile devices. The council is under no obligation to modify its systems to allow users to connect their personally-owned mobile devices to them where such modification may be required.

The council's IT contractors will provide IT support for personally-owned mobile devices, where this is necessary to enable users to access council information or council systems for business purposes.

The use of any mobile device to process and access council information creates risks including those relating to data protection, virus infection, copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and/or data. The risks are increased, and are also more difficult to manage, in the case of BYOD.

The council, its officers, Members and volunteers, are committed to processing all personal data in accordance with current UK Data Protection law, as specified within the council's Data Protection Policy, regardless of the device used to access the information. Users are required to keep council information and personal data secure. This applies equally to council information held on council systems and devices, or accessed/held on personally-owned mobile devices.

The council reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its information or ICT systems.

The council is the owner of all Chesham Town Council information and the contents

of Chesham Town Council systems together with everything which is created on, transmitted to, received on or printed from, or stored or recorded on each Mobile Device, in each case during the course of the council's business or otherwise on the council's behalf, irrespective of who owns that mobile device.

The council reserves the right to request access to inspect, or delete Chesham Town Council information held on a personally-owned mobile device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the council does not access the private information of the individual.

Monitoring of council ICT activity logs (relating to staff usage) whether using a council-issued mobile devices or personally-owned mobile devices, may be carried out in accordance with the Acceptable Use Policy.

User Responsibilities

Mobile Device Users are responsible for:

- The security of council information and of the device on which the information is held
- Storing council information on the mobile device only for so long as necessary
- Deleting council information from the mobile device when no longer required, or sooner if required by the council to delete it
- Ensuring where possible that the device has an up to date operating system and antivirus protection
- Complying with this policy and the related policies

Data Access and Storage

Use of any BYOD for council purposes is at the user's risk and the council is not liable for any losses, damages, or liability arising out of such use, including but not limited to loss, corruption or misuse of any content or loss of access to or misuse of such personally-owned mobile device, its software or its functionality.

When storing or processing confidential or sensitive information on a mobile device, use of a council issued mobile device should always be seen as the preferred mechanism. Storage using BYOD can put confidential information at risk of compromise and may be subject to varied technical standards and support, as well as access by third parties. Where BYOD is chosen over a council issued one for confidential or sensitive information, it should be authorised in writing by the relevant line manager.

Confidential or sensitive information should be stored within and accessed from council information systems and council managed storage to ensure security of and appropriate secure access to the information.

Confidential, sensitive or personal information should not be stored or transferred to

a Cloud computing service (such as personal SkyDrive or DropBox accounts) unless it is under a council negotiated contract.

Users should only store the minimum amount of information necessary to carry out the required task on a mobile device. A temporary cache may be held on the device, therefore any confidential, sensitive or personal information should be deleted from the device as soon as the information is no longer required.

Device and Physical Security

Information should be protected against loss or compromise when working remotely, for example at home or in public places.

Mobile devices accessing council information must have a strong (4 or more alphanumeric characters/pattern) passwords, passcode or PIN enabled to reduce opportunity for unauthorised access. These must be kept secure. The device should be set to automatically lock if inactive for 5 minutes or less, or locked manually using Ctrl, Alt and Delete keys.

Mobile devices used to access and or store confidential, personal or sensitive data should be subject to additional protection measures (such as encryption) to reduce opportunities for loss or compromise of the information.

Mobile devices should, where possible, have operating system and antivirus updates enabled. “Jailbroken” or “rooted” devices or those mobile devices which have otherwise circumvented the installed operating system security requirements (making them vulnerable to compromise) are not permitted to connect to the council’s ICT facilities.

Council-issued mobile devices must not be left unsecured whether on or off council premises. When unattended, the device must be locked (password, passcode or PIN protected) and the device should be secured with a recommended two barriers, i.e. limited access building or office and where possible a locked cupboard. There should be limited and controlled access to the cupboard keys, not left in cupboard or on a shelf.

Users must take responsibility for a mobile device and not leave it unattended in:

- Busy, public areas
- When travelling
- A car, including in its boot

Laptops must be carried as hand luggage when travelling.

The council’s IT contractors will ensure that council-issued mobile devices are not left unattended at any point in the delivery or installation process. This will include signed receipt of collection/delivery by the user.

Council-issued mobile devices must be uniquely identified, security-marked (where possible) and linked to a user. Records will be kept accurate and up to date.

Returning or Replacing a Council-issued Mobile Device
The devices are the property of the council and as such must be returned to the IT contractor upon change of user or termination of employment. They must not be sold, given away or otherwise disposed of by the user.

If devices are not returned (after a reminder process) the matter will be treated as a disciplinary matter. The matter may also be passed to the Police for consideration of further action or for recovery via civil litigation.

BYOD upon Termination of Employment or Device Replacement
Users must delete all council information from their device upon termination of their employment, or if the device is repaired, exchanged, sold, given away or otherwise disposed of. Users may be required to provide a written undertaking that this will be done. Without relieving users of their obligation to delete all council information, Chesham Town Council's rights under the above apply, including after termination of employment.

Costs Associated with Mobile Devices
In line with the Acceptable Use policy, council-issued mobile devices are provided for council business use.

The use of mobile devices overseas can lead to potentially significant costs, for example through data roaming, as well as risks to the device. Users must obtain approval for overseas travel with a council-issued mobile device.

There is currently no policy on the reimbursement of costs or data plans for BYOD.

Reporting Loss or Theft
In the event of loss or theft of any mobile device, irrespective of whether it is council-issued or personally-owned, the user must act promptly to minimise the risk of compromise to council information by immediately:

- Changing their council network log in password and notifying the IT contractors of the circumstances of the incident
- Changing any other passwords that may have been used on the device, e.g. banking
- Reporting theft of device to the Police
- Reporting loss or theft of mobile phone to the mobile network carrier directly

Appropriate steps will be taken to ensure that council information on or accessible from the mobile device is secured, including remote wiping of the mobile device. The remote wipe will destroy all council data on the mobile device. Although it is not intended to wipe other data that is personal in nature (such as photographs or

personal files or emails) it may not be possible to distinguish such information from council data in all circumstances. Users should, therefore, regularly backup all personal data stored on the mobile device.

REMOVABLE MEDIA POLICY

This refers to all types of computer storage which are not physically fixed inside a computer and includes the following:

- Memory cards, USB pens, etc.
- Removable or external hard disk drives
- Newer Solid State drives
- Mobile devices (iPod, iPhone, iPad, MP3 player)
- Optical disks, i.e. DVD and CD
- Floppy disks
- Backup tapes

The use of removable media is permitted where data is not personal, sensitive or confidential, e.g. a public presentation. Council-authorised, removable media can be used for personal, sensitive or confidential data subject to the removable media being encrypted to a recommended encryption standard of AES 256 and there being no other secure method of transferring data available.

Regularly updated Antivirus software should be present on all machines from which the data is taken from and machines on which the data is to be loaded.

Mobile devices and/or removable storage containing sensitive or highly sensitive data should not be sent outside of the council without prior written agreement from the relevant management team. The IT contractor should be consulted to ensure the level of security is appropriate for the type of data being transferred.

Data stored on removable media is the responsibility of the individual who operates the devices.

The user must note and accept that should their encryption password be forgotten, the removable device allows for a new password to be created, but this will involve formatting of the device and thus the total loss of the data. The removable device must therefore not be used to keep data that is not backed up securely in a central location.

Removable media should be physically protected against loss, damage, abuse or misuse when in use, storage and transit.

Mobile devices and or removable media that have become damaged should be given to the IT contractor to ensure it is disposed of securely to avoid data leakage.

When the business purpose has been satisfied, the contents of the removable media

should be removed from the media through a destruction method that makes recovery of the data impossible. Alternatively, the removable media and its data should be destroyed and disposed of beyond its potential reuse.

Wireless Internet Access

Members of the public who hire rooms at the Town Hall can also pay to access the Town Hall's wireless internet service. Hirers must agree to sign up to a set of conditions, including complying with our policy on Internet Access Unacceptable Behaviour, before being given access to the internet.

Wireless internet access is controlled by a password which can be changed by the Town Hall officers at any time.

POLICY REVIEW

Chesham Town Council is committed to reviewing its policies on a 4-year cycle and making improvements where possible. The policy will also be reviewed in the event of relevant changes in legislation and technology.

Adopted: 18 June 2018
Policy Due for Review: 18 June 2022